National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
for the
BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client

Report Number: CCEVS-VR-VID11640-2026
Dated: February 18, 2026
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Sheldon Durrant
Randy Heimann
Lisa Mitchell
Jaemond Reyes
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Khai Van
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This Validation Report (VR) documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy Client version 6.0 Client provided by BlackBerry Ltd. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation TOE by any agency of the U.S. government, and no warranty of the TOE is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in February 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements of the:

- *PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints*, Version 1.1, 31 May 2022 which includes:
    - Base PP: *Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14)
    - PP-Module: *PP-Module for Voice/Video over IP (VVoIP) Endpoints*, Version 1.0, 28 October 2020 (VVoIP10)
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 (PKGTLS11).

The TOE is the BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client. The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the *Common Methodology for IT Security Evaluation* (Version 3.1, Rev 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The Validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The technical information included in this report was obtained from the *BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client Security Target*, version 0.6, February 17, 2026 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE - the fully qualified identifier of the product as evaluated.
- The ST - describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The PP/PP-Modules to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client
Protection Profile	*PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints*, Version 1.1, 31 May 2022 which includes • *Base PP: Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14) • *PP-Module for PP-Module for Voice/Video over IP (VVoIP) Endpoints*, Version 1.0, 28 October 2020 (VVoIP10) *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 (PKGTLS11)
ST	*BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client Security Target*, version 0.6, February 17, 2026
Evaluation Technical Report	*Evaluation Technical Report for BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client*, version 0.3, February 17, 2026
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	BlackBerry Ltd.

Item	Identifier
Developer	BlackBerry Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Randy Heimann, Lisa Mitchell, Jaemond Reyes, Lori Sarem

3 Architectural Information

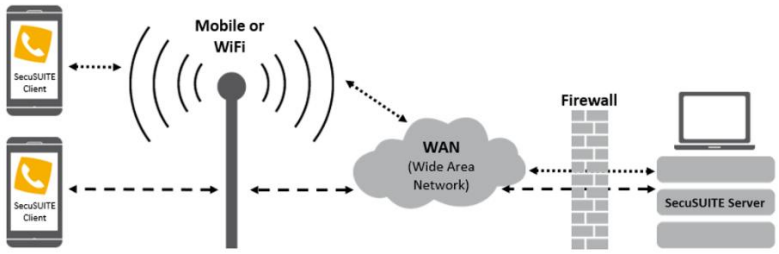
Note: The following architectural description is based on the description presented in the ST.

The TOE is BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client.

The TOE, herein referred to as the SecuSUITE/Envoy Client or the TOE, is a Voice over Internet Protocol (IP) (VoIP) application that executes on Android 14, iOS 17, and iPadOS 17 mobile device operating system.

3.1 TOE Description

The TOE is a VoIP application that executes on an evaluated mobile device operating system. As shown in the following figure, the TOE is part of the SecuSUITE Security Solution. The TOE does not work in isolation but relies on BlackBerry SecuSUITE Server components to enable secure VoIP communication.



User Context
The TOE user downloads the TOE from an app store (e.g., Apple Store, Google Play) and installs the app to their mobile device. On first use of the app, the user must go through a registration process in order to register to a specified BlackBerry SecuSUITE Server (identified by URI).

Once registered, the user can place secure VoIP calls using the app with largely the same interactions as with a normal phone call. The SecuSUITE Client provides encryption of user call signaling and voice data.

Users are typically invited to join SecuSUITE/Envoy service via an activation email initiated by their corporate IT administrator who adds users via the BlackBerry SecuSUITE Server administration portal. The activation email includes the activation credentials as well as the option to scan a QR code to initiate the registration with the SCA server.

VVoIP Client
The SecuSUITE Client establishes a secure tunnel for voice communications with another SecuSUITE/Envoy client or the SecuSUITE Server. The tunnel provides confidentiality, integrity, and data authentication for information that travels across the public network. This occurs using the Secure Real-Time Transport Protocol (SRTP) that has been established using the Session Description Protocol (SDP) and the Security Descriptions for Media Streams (SDES) for SDP – the TOE supports SDES-SRTP.

The TOE Client also protects communications between itself and the SIP Server by using a Transport Layer Security (TLS)-protected signaling channel. To register the TOE within the domain, the TOE is required to be password authenticated by the SIP Server. The TOE also makes use of certificates to authenticate both the SIP server end and the TOE itself through the TLS connection.

Group/Conference Calls

Besides the peer-to-peer calls between two instances of the TOE, the SecuSUITE/Envoy solution also allows the setup of a secure conference call between a group of SecuSUITE users. For that, individual calls and trusted channels are established between all TOEs participating in the group call (for a group call between 4 participants, every TOE has 3 individual calls to the members of the group). The individual SIP and SRTP connections are established exactly the same way the peer-to-peer calls are setup via the SecuSUITE Server. They are encrypted end-2-end and the individually decrypted audio streamed is mixed only locally by each client so that no clear text representations of the audio streams exist in a central component.

Secure Text Messaging

The TOE client allows encrypted instant message transfer between client applications. Secure Text Messaging utilizes the same TLS protected communication channel that is used during initial SCA registration used to transfer client configuration settings and SIP credentials between SecuSUITE Server and client.

Group Messaging

Besides the peer-to-peer text messaging between two instances of the TOE, the SecuSUITE/Envoy solution also allows the setup of messaging groups between an arbitrary number of SecuSUITE users. The messages are individually encrypted for all TOE users participating in the group messaging session the same way peer-to-peer messages are protected.

Calls Destined Beyond the SecuSUITE Server

The TOE always encrypts the user's call signaling and data (voice) transmitted to other TOE VoIP endpoints registered with the SecuSUITE Server and transmitted to the SecuSUITE Server itself. The SecuSUITE Server administrator can configure calling to additional endpoints which are reached through a PBX (another SIP server connected to local/internal landline phones and potentially connected to outside phone lines). If configured, the TOE can then place calls to additional endpoints beyond the SecuSUITE Server through the configured PBX; however, because the call signaling and call data travels beyond the SecuSUITE Server itself, its security lies beyond the TOE and SecuSUITE Server's control.

While the ability of the SecuSUITE Server to route calls to additional endpoints through a PBX lies beyond the scope of this ASPP14/PKGTLS11/VVoIPAS10 evaluation, the TOE can indicate when a user's call travels beyond the SecuSUITE Server.

The SecuSUITE Server allows an administrator to configure (refer to BlackBerry SecuSUITE Server evaluation VID11634 against the Enterprise Session Controller Protection Profile) which phone number prefixes the administrator deems "land secure" and which calls "breakout" to external phone lines (with unknown security). By default, the SecuSUITE Server treats all calls routed to the PBX as "breakout" calls. These designations cause an image indicating this disposition of the call to appear on the TOE's User Interface (UI) as described in the Common Criteria Configuration Guide. Again, while beyond the scope of this evaluation, the concepts of

"Secure Landing" and "Breakout Calls" are useful for TOE users to understand, in the event that their administrator has configured their SecuSUITE Server to route calls to additional endpoints through a PBX.

Envoy Client
The Envoy Client is a branded version of the SecuSUITE client that is identical from a functional and security implementation perspective. The Envoy client is distributed by BlackBerry and differs basically in the used UI assets and product publishing.

3.2 TOE Evaluated Platforms

Details regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The TOE is compromised of the SecuSUITE version 6.0 and Envoy version 6.0.

Before a SecuSUITE client can exchange messages with the SIP Server, the SecuSUITE Client must be registered to SecuSUITE and to the BlackBerry SecuSUITE Server (also referred to as the Enterprise Session Controller, or ESC) via the SCA Server. Once properly registered, the Client can initiate or receive a "Call". Call data is exchanged with a VVoIP endpoint through SecuSUITE Server which provides an SRTP proxy. The ESC is also referred to as the SIP server. Additional information on the process for Client registration to the SecuSUITE server can be found in the ST.

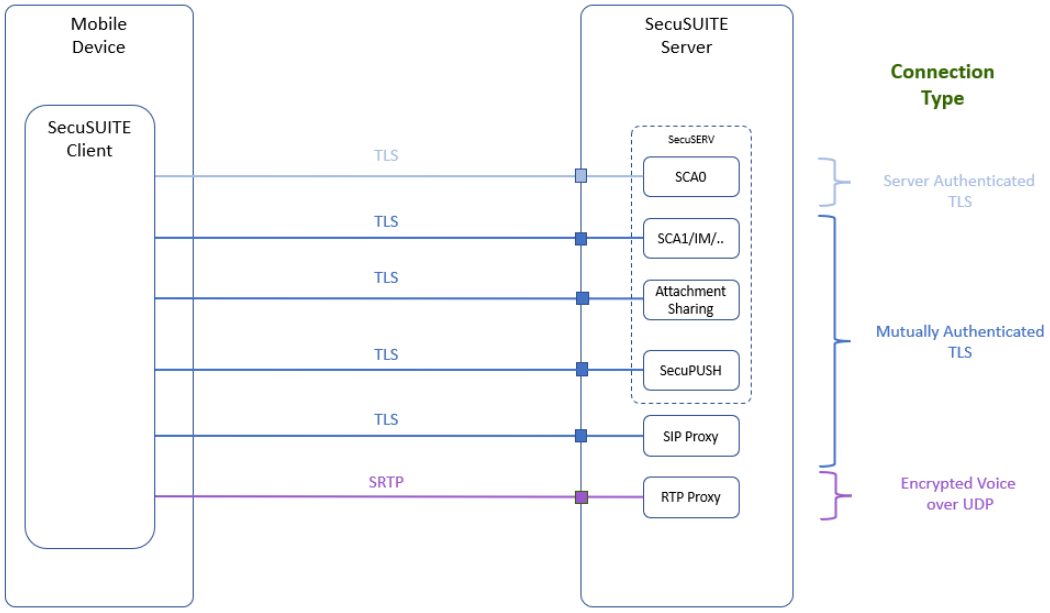
The client registers with the SIP server every time a new connection with the SIP server is established. That is, after:

- Client app was installed and SCA procedure was successfully passed, or
- Client was restarted, or
- Client had lost TLS connection to SIP server (e.g. because of network change or problems)

Additional information on the process for registering with the SIP server, call setup, and call termination can be found in the ST.

3.4 Physical Boundaries

The TOE boundary and communication with the SecuSUITE Server is illustrated in the figure below.



The TOE is part of the SecuSUITE security solution and requires the following components to be present in the environment:

a) SecuSUITE SCA Server. The SCA Server authenticates users and facilitates VoIP client enrollment and pushes client SIP configuration to the client.

b) SecuSUITE SIP Server. The SIP Server is used to establish the secure connection between the mobile devices. The use of a TLS connection, providing encryption and mutual authentication, ensures that the devices connect with authorized SIP servers only and the dialed call numbers are transmitted encrypted.

c) SecuSUITE RTP Proxy. The Real-Time Transport Protocol (RTP) Proxy bridges media packets sent between clients. The RTP Proxy is part of the SecuSUITE SIP Server. The SIP Server creates and deletes RTP and Real-Time Transport Control Protocol (RTCP) bridging sessions in the RTP Proxy.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Communication
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security management
6. Privacy
7. Protection of the TSF
8. TOE access
9. Trusted path/channels

4.1 Communication

The TOE utilizes the Opus codec by default to transmit voice media. The Opus codec utilizes a fixed bit-rate.

4.2 Cryptographic support

The TOE includes its own cryptographic module to perform operations in support of authentication actions and network communications using the TLS and SRTP protocol. The TOE implements TLS version 1.2 with mutual authentication using elliptic-curve cryptography. The TOE also relies upon its platform for certain cryptographic operations, including providing random data to seed the TOE's own DRBG. The TOE relies upon the platform (i.e., iOS, iPadOS, and Android) cryptographic libraries for operations related to protecting keys in platform offered storage (i.e., a key store).

4.3 User data protection

The TOE enforces the media transmission policy when communicating with remote VVoIP endpoints which use TLS and SRTP protocols. The TOE also ensures that communication with an SCA server is protected using TLS. The TOE protects user data by utilizing platform services for data storage.

4.4 Identification and authentication

The TOE authenticates TLS peers using X.509v3 certificates. It performs extensive X.509 certificate validation checks on these certificates, rejecting invalid or revoked certificates.

4.5 Security management

The TOE receives configuration settings during its registration with an SCA server. The client allows management operations that specify the SIP server to be used for connections.

4.6 Privacy

The TOE does not transmit Personally Identifiable Information over any network interfaces.

4.7 Protection of the TSF

The TOE relies on the physical boundary of the evaluated platform as well as the Android and iOS/iPadOS operating systems for the protection of the TOE's application components.

The TOE relies upon these platforms to indicate the current TOE version. If an update is needed, it is obtained from the platform's application store. The TOE's software is digitally signed in accordance with the requirements of each application store.

The native Apple and Android cryptographic library, which provides some of the TOE's cryptographic services, have built-in self-tests that are run at client start-up to ensure that the algorithms are correct. If any self-tests fail, the TOE will not be able to perform its cryptographic services. The TOE includes its own cryptographic library that also includes self-tests that are run when the client starts.

4.8 TOE access

The TOE includes a 15 second default timeout that can terminate idle voice/video transmission. This timeout value can be changed by the configuration obtained from the SCA server.

4.9 Trusted path/channels

The TOE encrypts all data transmitted with an ESC and another VVoIP endpoint using TLS to protect HTTPS, SIP and SRTP communications. The TLS channel established with an ESC or VVoIP endpoint can be used to exchange SIP messages or to initiate the use of SRTP for voice/video traffic.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14)
- *PP-Module for PP-Module for Voice/Video over IP (VVoIP) Endpoints*, Version 1.0, 28 October 2020 (VVoIP10)
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 (PKGTLS11)

That information has not been reproduced here and the ASPP14/VVoIP10/PKGTLS11 should be consulted if there is interest in that material.

5.2 Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14/VVoIP10/PKGTLS11 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the *Application Software Protection Profile* with the *PP-Module for Voice and Video over IP* and the *TLS Package* and performed by the Evaluation team).
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The TOE consists solely of software and relies on its operational environment for supporting security functionality, as identified in the ST.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP14/VVoIP10/PKGTLS11 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *SecuSUITE 6.0 Common Criteria Guide*, Version 2 10a, Release 6.0

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary *Detailed Test Report for BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client*, Version 0.3, February 17, 2026 (DTR), as summarized in the evaluation *Assurance Activity Report for BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client*, Version 0.3, February 17, 2026 (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the ASPP14/VVoIP10/PKGTLS11 including the tests associated with optional requirements. The AAR, in section 3.4.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The TOE is BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client.

The TOE executes on the following mobile devices[1]:

1. Samsung – Android 14
    a. North America (Qualcomm Snapdragon 8 Gen 3)
        i. Galaxy S24 Ultra 5G
        ii. Galaxy S24+ 5G
        iii. Galaxy S24 5G
        iv. Galaxy S23 FE
        v. Galaxy Tab S8/S8+/S8 Ultra
    b. North America (Qualcomm Snapdragon 8 Gen 2)
        i. Galaxy S23 Ultra 5G
        ii. Galaxy S23+ 5G
        iii. Galaxy S23 5G
        iv. Galaxy Tab S9/S9+/S9 Ultra
        v. Galaxy Z Flip5 5G
        vi. Galaxy Z Fold5 5G
    c. North America (Qualcomm Snapdragon 8 Gen 1)
        i. Galaxy S22 Ultra 5G
        ii. Galaxy S22+ 5G
        iii. Galaxy S22 5G
        iv. Galaxy Z Fold4 5G
        v. Galaxy Z Flip4 5G
    d. North America (Qualcomm Snapdragon 750G)
        i. Galaxy A52 5G
    e. International (Samsung Exynos 2400)
        i. Galaxy S24 5G
        ii. Galaxy S24+ 5G
    f. International (Samsung Exynos 2200)
        i. Galaxy S23 FE
        ii. Galaxy S22 5G
        iii. Galaxy S22+ 5G
        iv. Galaxy S22 Ultra 5G
2. Apple iPhone – iOS17
    a. A15 Bionic
        i. iPhone SE (3rd gen)
        ii. iPhone 13
        iii. iPhone 13 Mini
        iv. iPhone 13 Pro
        v. iPhone 13 Pro Max
        vi. iPhone 14

[1] Note the list of equivalent devices is taken from the evaluated devices' Security Targets.

vii. iPhone 14 Plus

b. Apple A16 Bionic
   i. iPhone 14 Pro
   ii. iPhone 14 Pro Max
   iii. iPhone 15

c. Apple A17 Pro
   i. iPhone 15 Pro
   ii. iPhone 15 Pro Max

3. Apple iPad – iPadOS17
   a. Apple M2
      i. iPad Pro 11 inch (4th Gen)
      ii. iPad Pro 12.9 inch (6th Gen)
      iii. iPad Air 11 inch (6th Gen)
      iv. iPad Air 13 inch (6th Gen)

The evaluation tested on the Samsung Galaxy S23, Apple iPhone 13, and Apple iPad Air (6th generation).

The mobile devices have been NIAP certified as follows:

Samsung Galaxy Devices on Android 14 (VID11444):

https://www.niap-ccevs.org/products/11444

Samsung Galaxy Devices on Android 14 (GalaxyA52 5G and Galaxy A42 5G only) (VID11539): https://www.niap-ccevs.org/products/11539

Apple iOS 17: iPhones (VID11446) https://www.niap-ccevs.org/products/11446

Apple iPadOS 17: iPads (VID11447): https://www.niap-ccevs.org/products/11447

Note that the iPad Air 11 inch (6th Gen) and iPad Air 13 inch (6th Gen), while not listed on VID11447 are equivalent devices due to having the same processor

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5 and the specific evaluation activities specified in ASPP14/VVoIP10/PKGTLS11. The evaluation determined the BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client TOE to be Part 2 extended and Part 3 extended, and to satisfy the requirements specified in the ASPP14/VVoIP10/PKGTLS11.

9.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions and meets the requirements specified in the claimed Protection Profile for design evidence. The design documentation consists of a functional specification contained in the Security Target and Guidance documents providing descriptions of the TOE external interfaces. Additionally, the Evaluation team performed the assurance activities specified in the ASPP14/VVoIP10/PKGTLS11 related to the examination of the information contained in the TSS.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The Evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in

the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the ASPP14/VVoIP10/PKGTLS11 and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities was last performed on February 11, 2026.

The Evaluation team searched the following databases:

- MITRE CVE Database (https://www.cve.org/),
- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
- CVE details (https://www.cvedetails.com/vulnerability-search.php), and
- Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

with the following search terms:

"SecuSUITE", "Boost", "zlib", "openssl", "pjproject", "poco", "libphonenumber", "icu", "protobuf", "opus", "silk", "libsrtp2", "sqlite3", "abseil", "secucore", "secuintegritycheck",

"secuwebrtc", "androidx", "facebook", "bumptech glide", "photoview", "datatransport", "android material", "android gms", "app-update", "core-common", "errorprone", "firebase", "listenablefuture", "zxing", "okio", "commons-codec", "javax", "joda-time", "androidannotations", "jetbrains", "jspecify", "blackberry", "blackberry envoy", "cryptocomply", "clang", "sipenginewrapper", "libsecu", "jsonrpc", "srp", "mlspp", "nsdata+base64url", "uiimage+imageeffects", "crasheye", "spongycastle", "pdfbox", "robolectric", "objenesis", "mockito", "stax-ex", "glassfish", "hamcrest", "codehaus", "checkerframework", "kxml2", "jcip", "jna", "bytebuddy", "junit", "jakarta", "perfmark", "commons-io", "fastinfoset", "istack", "jcodemodel", "juniversalchardet", "testing platform", "j2objc", "guava", "errorprone", "tink", "gson", "findbugs", "google auto", "annotations", "desugar jdk", "android common", "android utp", "android tools", "android databinding", "webkit", "usernotifications", "uniformtypeidentifiers", "swiftui", "apple security", "quicklookthumbnailing", "apple photos", "apple network", "localauthentication", "developertoolssupport", "coremedia", "coreimage", "coregraphics", "apple combine", "apple callkit", "audiotoolbox", "avkit", "avfaudio", "backgroundtasks", "apple accelerate", "apple systemconfiguration", "imageio", "apple uikit", "apple contacts", "coretelephony", "cfnetwork", "avfoundation", "assetslibrary", "apple foundation", "apple pushkit", "corefoundation", "coreservices", "quartzcore", "libc.so", "libdl.so", "libm.so", "libopensles.so", and "liblog.so".

The BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client evaluation included the Vendor submission of a Software Bill of Materials (SBOM) for analysis, per NIAP policy. The SBOM provided a comprehensive listing of the third-party library components contained in the TOE. The SBOM was used in the vulnerability analysis during the evaluation period and was updated by the Vendor as requested by NIAP.

The conclusion drawn from the vulnerability analysis is that no residual TOE vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The Validation team’s assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the configuration instructions in the Guidance document defined in Section 6. No other versions of the TOE software, either earlier or later, were evaluated.

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST and only that functionality was evaluated. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

The Validation team strongly recommends that all TOE platforms in the operational environment are kept up to date with patches as they are released. In addition, Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client Security Target*, Version 0.6, February 17, 2026.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this VR:

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, April 2017.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.

[4] *Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14).

[5] *PP-Module for PP-Module for Voice/Video over IP (VVoIP) Endpoints*, Version 1.0, 28 October 2020 (VVoIP10).

[6] *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 (PKGTLS11).

[7] *SecuSUITE 6.0 Common Criteria Guide*, Version 2 10a, Release 6.0 (AGD)

[8] *BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client Security Target*, Version 0.6, February 17, 2026 (ST).

[9] *Assurance Activity Report for BlackBerry SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client*, Version 0.3, February 17, 2026 (AAR).

[10] *Detailed Test Report for SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client*, Version 0.3, February 17, 2026 (DTR).

[11] *Evaluation Technical Report for SecuSUITE version 6.0 and BlackBerry Envoy version 6.0 Client*, Version 0.3, February 17, 2026 (ETR).